CLAIMS

What is claimed is:

1. A policy-based network security management system, the system comprising:
a security management controller comprising one or more processors;
a computer-readable medium carrying one or more sequences of instructions for policy-based network security management, wherein execution of the one or more sequences of instructions by the one or more processors causes the one or more processors to perform the steps of:
receiving a set of data regarding a user of a network;
automatically deciding on a course of action based on the set of data, wherein the course of action may be adverse to the user although the set of data is insufficient to establish whether the user is performing a malicious action; and
sending signals to one or more network elements in the network to implement the decision.

2. The system of claim 1, wherein the set of data includes at least one or more alerts related to the user.

3. The system of claim 1, wherein the signals include multiple alerts generated by multiple users; and the system further comprising sequences of instructions for correlating the multiple alerts to the multiple users.

4. The system of claim 1, wherein the set of data is a first set of data that is collected over a first duration of time; and the system further comprising sequences of instructions for collecting a second set of data over a second duration of time, wherein the first duration of time is shorter than the second duration of time.

5. The system of claim 4 further comprising sequences of instructions for performing the steps of:

assessing a risk level of the user harming the network based on the second set of data, wherein the second duration of time is sufficient to collect historical data regarding past malicious activities of the user; and

assessing a current alert level based on the first set of data, wherein the first duration of time is of a length appropriate for assessing current activities of the user.

6. The system of claim 1 or 5, further comprising sequences of instructions for performing the steps of:

receiving signals related to an external source including at least an alert assessment relevant to the network as a whole; and

creating and storing a current alert level value based on the alert assessment.

7. The system of claim 1, further comprising sequences of instructions for performing the steps of:

receiving signals carrying performance information related to a health level of the network; and

determining the course of action based at least in part on the set of data and the performance information.

8. The system of claim 1 further comprising:

a plurality of routers for routing information sent by users and servers to a variety of destinations;

a subscriber management system for managing a network;

a controller for executing the sequences of instructions;

a network element for generating input for the set of data; and

sequences of instructions for sending signals to the network elements.

9. A computer-readable medium carrying one or more sequences of instructions for providing policy-based network security management, wherein execution of the one or more sequences of instructions by one or more processors causes the one or more processors to perform the steps of:

receiving signals carrying network performance information regarding health of a network and resource performance information regarding health of resources used by a network;

assessing a health level based on the network performance information and the resource performance information; and

sending signals carrying information affecting use of the network based on at least the health level.

10. A computer-readable medium as recited in claim 9, further comprising the steps of:

receiving signals related to one or more alerts;

associating with the user at least the one or more alerts within a current alert dataset that establishes a current alert level for the user.

11. A computer-readable medium as recited in claim 9, further comprising the step of establishing a user alert.

12. A computer-readable medium as recited in claim 9, further comprising the steps of:

receiving signals related to one or more alerts;

associating with a user at least the one or more alerts within a historical dataset of alert related information that establishes a user risk level for the user.

13. A computer-readable medium as recited in Claim 9, wherein the step of sending signals further comprises the steps of:

deciding on a course of action based on at least a user risk level, a current alert level, and the health level, and

wherein the information affecting the use of the network based on at least the health level is based on at least the course of action and is based on the health level as a result of being based on the course of action.

14. A computer-readable medium as recited in claim 10, wherein the deciding step includes at least

determining a user risk state from a user risk level, determining a current alert state from a current alert level, and determining a health state from the health level; and

wherein the information affecting the use of the network is based on at least the health level as a result of being is based on at least the user risk state, the current alert state, and the health state.

15. A policy-based network security management system, the system comprising:

a security management controller comprising one or more processors; and the computer readable medium of claim 9.

16. A method of providing policy-based network security management, comprising the steps of:

receiving a set of data regarding a user of a network;

automatically deciding on a course of action based on the set of data, wherein the course of action may be adverse to the user although the set of data is insufficient to establish whether the user is performing a malicious action; and

sending signals to one or more network elements in the network to implement the decision.

17. The method of claim 16 wherein the set of data includes at least one or more alerts related to the user.

18. The method of claim 16, wherein the signals include multiple alerts generated by multiple users, and the method further comprises correlating the multiple alerts to the multiple users.

19. The method of claim 16, wherein the set of data is a first set of data, which was collected over a first duration of time, and the method further comprising the step of collecting a second set of data over a second duration of time, wherein the first duration of time is significantly shorter than the second duration of time.

20. The method of claim 19, wherein the second set of data is used to assess a risk level of the user harming a network, and the second duration of time is sufficient to collect historical data regarding past malicious activities of the user; and the first set of data is used to assess a current alert level, and the first duration of time is of a length appropriate for assessing current activities of the user.

21. The method of claim 19 further comprising receiving signals related to an external source including an alert assessment relevant to the network as a whole, wherein the current alert level is also based on the alert assessment.

22. The method of claim 16 further comprising receiving signals carrying performance information related to a health level of the network, wherein the course of action is based on the set of data and the performance information.

23. A method of policy-based network security management, comprising the computer-implemented steps of:

receiving one or more signals carrying network performance information regarding health of one or more network devices in a network, and resource

performance information regarding health of one or more resources used by the network;

assessing an overall network health level based on the network performance and the resource performance; and

sending signals carrying information affecting use of the network based on the overall network health level.

24. The method of claim 23 further comprising:

receiving signals related to one or more alerts;

including at least the one or more alerts within a historical dataset of alert related information that establishes a user risk level for a user; and

including at least the one or more alerts within a current alert dataset that establishes a current alert level.

25. The method of claim 23, wherein the sending step further comprising the steps of:

deciding on a course of action based on at least a user risk level, a current alert level, and the overall network health level, and

the information affecting the use of the network includes at least information for carrying out the course of action.

26. The method of claim 23, wherein the deciding step includes at least the steps of:

determining a user risk state from a user risk level;

determining a current alert state from a current alert level; and

determining a health state from the overall network health level; and

wherein the information affecting the use of the network is based on at least the health level as a result of being based on at least the user risk state, the current alert state, and the health state.

27. A method of policy-based network security management, comprising the computer-implemented steps of

collecting network performance statistics related to an overall health of a network and individual performance statistics of one or more individual units of the network, the collecting being performed by a performance management system;

sending the performance statistics to a controller for analysis;

computing an overall health state from a health level based on the network performance statistics and the individual performance statistics, using the controller;

reading external alert data from an external alert source, using the controller;

collecting security event data from the network;

sending the security event data to a fault management system;

using the fault management system for

checking for duplications in the security event data, and

deduplicating duplicate security events in the security event data;

calculating an alert state from an alert level based on the security event data from the fault management system and the external alert data;

obtaining user information from a subscriber management system;

correlating the security event data from the fault management system with the subscriber information to form correlated security event data;

reading external user risk data from an external user risk source into the controller;

calculating a user risk state from a user risk level based on the correlated security event data and from the external user risk data, using the controller;

calculating a decision regarding whether to take corrective action based on the overall health state, the alert state, and the user risk state, using the controller;

sending the decision from the controller to the subscriber management system; and

sending directives, related to the decision, from subscriber management system to the network.

28. A system comprising:

a fault managements system for

receiving network security data and

deduplicating duplicate indications of security events in the network security data to form deduplicated security event information;

a subscriber management system for managing subscribers using a network,

the subscriber management system

having user information data about individual users and

being capable of sending directives to individual users based on a decision to take corrective action toward the individual users;

wherein the deduplicated network security data from the fault management system is correlated to the subscriber information to form correlated network security data;

a performance management system for receiving

overall performance data related to an overall health of a network and

individual performance data related to a health of one or more individual units of the network;

a controller for

receiving

external alert data from an external alert source,

external user risk data from an external user risk source,

the deduplicated network security event information,

the correlated network security information,

the overall performance data, and

the individual performance data, and

computing

an alert state from an alert level based on at least the external alert data and the deduplicated network security event data,

a user risk state from at least the external user risk data and a user risk level based on the correlated network security event data,

a health state from a health level based on at least the overall performance data and the individual performance data, and

the decision whether to take corrective action based on at least the alert state, the user risk state, and the health state, and

causing directives that implement the decision to be sent to the network .